

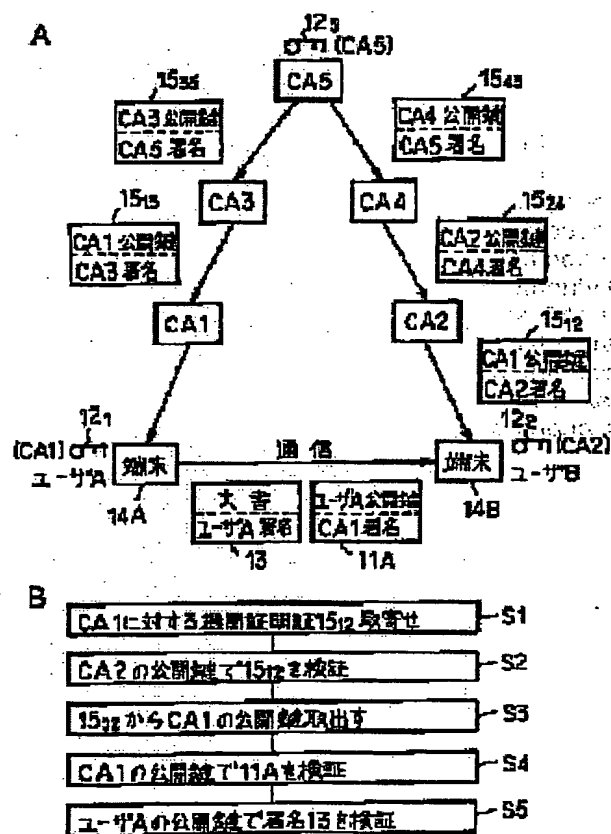
PUBLIC KEY AUTHENTICATION METHOD

Patent number: JP10215245
Publication date: 1998-08-11
Inventor: HASHIMOTO SHOICHI
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
 - International: H04L9/32
 - european:
Application number: JP19970015463 19970129
Priority number(s): JP19970015463 19970129

Report a data error here

Abstract of JP10215245

PROBLEM TO BE SOLVED: To relieve the load of the user for authentication processing in the case that a certification authority issuing a public key certificate is different from the certification authority issuing the certificate for the user. **SOLUTION:** Once a certificate 11A authenticated by a certification authority CA1 has been received, a user B whose public key has been authenticated by a certification authority CA2 requests the authentication of the CA1 to the CA2. The CA2 traces the trusted tree structure of the CA1 and authenticates the validity of a signature in a certificate 1535 with respect to a certification authority CA3 by using a public key of a certification authority CA5 that is the highest certification authority, authenticates the validity of a signature in a certificate 1515 with respect to the certification authority CA1 by using a public key of the certification authority CA3. When the signature is successfully authenticated, the CA2 puts its public key as signature to the public key of the CA1 in the certificate 1513, sends a certificate 1512 to the user B. The user B uses the public key of the CA2 to authenticate the certificate 1512. When the signature is successfully authenticated, the user B uses the public key included in the certificate to authenticate a public key of a user A in the certificate 11A.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁(JP)

(12)公開特許公報 (A)

(11)特許出願公開番号

特開平10-215245

(43)公開日 平成10年(1998)8月11日

(51)Int. Cl.⁶

H04L 9/32

識別記号

F I

H04L 9/00 675 Z
675 D

審査請求 未請求 請求項の数3

O L

(全6頁)

(21)出願番号 特願平9-15463

(22)出願日 平成9年(1997)1月29日

(71)出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72)発明者 橋本 正一

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

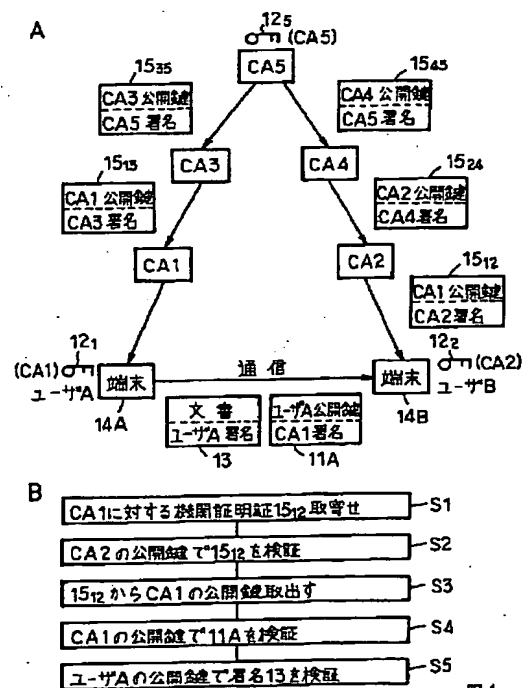
(74)代理人 弁理士 草野 卓

(54)【発明の名称】 公開鍵認証方法

(57)【要約】

【課題】 公開鍵証明証を発行した証明機関が異なる場合のユーザの検証処理を軽減する。

【解決手段】 証明機関CA2により公開鍵を証明されているユーザBがCA1により証明された証明証11Aを受信すると、CA2にCA1の検証を依頼する。CA2はCA1の信頼関係木構造を辿って、最上位のCA5の公開鍵でCA3に対する証明証15₃₅の署名の正当性を検証し、CA3の公開鍵でCA1に対する証明証15₁₃の署名の正当性を検証し、これらに合格すると15₁₃中のCA1の公開鍵をCA2の公開鍵で署名して証明証15₁₂をユーザBへ送り、ユーザBは、CA2の公開鍵で15₁₂を検証し、合格したらこれに含まれているCA1公開鍵を用いて証明証11AのユーザAの公開鍵を検証する。



【特許請求の範囲】

【請求項 1】 公開鍵とその所有者との対応付けを保証して、公開鍵証明証を発行する証明機関が複数存在し、これら証明機関が木構造などの信頼関係により上位の証明機関がその下位の証明機関の公開鍵を保証した機関証明証を発行することを順次行っており、利用者 B の端末（以下端末 B と記す）に受信された利用者 A の公開鍵証明証 A の発行証明機関 A が、端末 B（利用者 B）に対する公開鍵証明証 B の発行証明機関 B と異なる場合に、端末 B は証明機関 B に証明機関 A を保証する機関証明証の発行を依頼し、証明機関 B はその機関 B が証明機関 A の公開鍵を保証した機関証明証を端末 B に送り、端末 B は受信した機関証明証を検証し、合格すると、その機関証明証に含まれている証明機関 A の公開鍵を用いて上記公開鍵証明証 A の検証を行うことを特徴とする公開鍵認証方法。

【請求項 2】 上記証明機関 B は上記証明機関 A の公開鍵を保証した機関証明証の発行に際し、上記証明機関 A の公開鍵をその上位の証明機関が保証した機関証明証により証明機関 A の信頼性を検証し、この証明機関の信頼性の検証を順次上位の証明機関に対して行い、最上位の証明機関による保証の確認ができた場合に上記証明機関 A の公開鍵を保証した機関証明証を発行することを特徴とする請求項 1 記載の公開鍵認証方法。

【請求項 3】 上記証明機関の信頼性の認証が正しい場合にその入手した各機関証明証及び上記証明機関 A に対して発行した機関証明証を記憶しておき、上記端末 B の機関証明証の発行依頼に対し、上記記憶した機関証明証を利用することを特徴とする請求項 2 記載の公開鍵認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は公開鍵暗号方式を用いた情報通信において、異なる証明機関から証明証が発行されているユーザ（利用者）間で通信を行う場合に、通信相手の証明証の正当性を効率的に確認し、安全に通信を行うための認証方法に関するものである。

【0002】

【従来の技術】電子情報の送受信において、確かに送信者本人から送信されたものであるかということや、通信路において改ざんが行われていないかということなどを検知するための方法として公開鍵暗号方式が利用されている。この方式では、一般に広く公開しておく公開鍵と、自分のみが知り得る秘密鍵の 2 種類の鍵を用いて通信が行われる。ここで公開鍵を単に周知するだけでは他人を装って通知する「なりすまし」と呼ばれる脅威が考えられることから、証明機関が、公開鍵と所有者との関係を保証し、所有者の公開鍵証明証を発行する形態が一

般に行われている。証明証には、ユーザ（利用者）の公開鍵および所有者に関する情報と、証明証を発行する証明機関の電子署名（以下 CA 署名と略す、CA: Certification Authority）が付与されている。ユーザは、この証明機関の公開鍵を用いて通信相手の証明証の CA 署名を復号化処理することで、確かに当該証明機関が発行した証明証であることを検証し、通信相手の証明証に登録されている公開鍵を取り出して利用する。

【0003】ここで検証に用いる証明機関の公開鍵は、通常、証明機関が証明証を発行したユーザに対して、安全な方法で配付されているため、同一の証明機関から証明証の発行を受けたユーザ同士が通信する場合には、配付されている証明機関の公開鍵によって通信相手の証明証の正当性を検証することができる。即ち図 3 に示すように、ユーザ A は利用する公開鍵とその所有者がユーザ A であることを証明機関 CA 1 により署名したユーザ A の公開鍵証明証 11A を発行してもらう。ユーザ B も同様にユーザ公開鍵とその所有についての署名をしたユーザ B の公開鍵証明証 11B を証明機関 CA 1 により発行してもらう。同時にユーザ A、ユーザ B に、証明証検証用の証明機関 CA 1 の公開鍵 12₁ がそれぞれ安全な方法で配付されている。ユーザ A がユーザ A の署名を付けた文書 13 をユーザ B へ送信する際に、まずユーザ A の公開鍵証明証 11A をユーザ A の端末 14A からユーザ B の端末 14B へ送信する。ユーザ B の端末 14B では受信した証明証 11A を、証明機関 CA 1 の公開鍵 12₁ によりそのユーザ A の公開鍵が証明機関 CA 1 により認証されたものであるか否かを検証し、つまり公開鍵 12₁ で証明機関 CA 1 の署名を復号化して公開鍵を復号し、その復号した公開鍵が、証明証 11A に示されているユーザ A の公開鍵と同一であることを調べ、一致していれば、その公開鍵は証明機関 CA 1 によりユーザ A のものであると保証されたものとして、その公開鍵を取り出して文書 13 の署名を検証する。

【0004】しかしながら、異なる証明機関から証明証が発行されているユーザ間で通信を行う場合には、通信相手の証明証に付与された CA 署名を検証するための証明機関の公開鍵を持っていないため、通信相手の証明証の正当性を確認することができない。そこで通信相手の証明証を発行した証明機関が信頼できる証明機関であるかを確認するために、図 4 に示すように、上位の証明機関が下位の証明機関に対して証明証を発行することで、複数証明機関間における信頼関係の木構造を構築する。そして、「信頼できる証明機関が信頼している証明機関は信頼できる」という考えに基づいて、相手証明機関から、信頼の木構造を複数の証明機関を介しながら木構造全体から信頼されている最上位の証明機関 CA 5 まで辿ることによって、相手証明機関の信頼性が確認できるようになる。

【0005】例えば図 4 A に示すように、ユーザ A の公

開鍵に対する証明証 11A を発行した証明機関 CA1 の上位の証明機関 CA3 は証明機関 CA1 の公開鍵とその機関名 CA1 と、これに対する CA3 の署名とよりなる機関証明証 15₁₃ を発行し、証明機関 CA3 の上位の証明機関 CA5 は証明機関 CA3 の公開鍵およびその機関 CA3 と、これらに対する CA5 の署名とよりなる機関証明証 15₃₅ を発行する。証明機関 CA5 はこの例では最上位の機関である。同様にユーザ B に対し、公開鍵証明証 11B を発行した証明機関 CA2 に対し、その上位の証明機関 CA4 は機関証明証 15₂₄ を発行し、証明機関 CA4 に対し、その上位証明機関 CA5 が機関証明証 15₄₅ を発行し、木構造の信頼関係が構成されている。

【0006】ユーザ 14A がその署名付き文書 13 をユーザ B へ送る際に、ユーザ A の公開鍵証明証 11A をユーザ B へ送信しても、ユーザ B の端末 14B は証明機関 CA2 の公開鍵 12₂ しかもっていないから証明証 11A の正当性を検証することはできない、つまりユーザ A の公開鍵が信頼できるものか不明である。従ってユーザ B の端末 14B は図 4B に示すように受信した証明証 11A の公開情報からその証明機関 CA1 とその上位機関 CA3 を知り、上位機関 CA3 が証明機関 CA1 に対し発行した機関証明証 15₁₃ の正当性を証明機関 CA3 の公開鍵で検証し、これに合格すれば、証明機関 CA3 の上位機関 CA5 が証明機関 CA3 に対して発行した機関証明証 15₃₅ の正当性を機関 CA5 の公開鍵 12₅ で検証し、この検証に合格したら、証明機関 CA3, CA1 がそれぞれ信頼されるものであり、従って証明証 11A のユーザ A の公開鍵も信頼できるものと判定する。

【0007】このように信頼性の確認の際には、木構造を辿る際に証明機関間で発行されている証明証を取り寄せて、下位証明機関の証明証に付与されている上位証明機関の署名を、その上位証明機関の証明証中にある公開鍵によって検証するということを順次最上位の証明機関 CA5 の公開鍵による検証が行われるまで繰り返し行うことによって、相手証明機関 CA1 の公開鍵の正当性を確認していた。

【0008】

【発明が解決しようとする課題】自己の公開鍵証明証を発行している証明機関と異なる証明機関から発行されている通信相手の証明証の正当性を検証する場合、図 4 に示したように、証明機関間の信頼関係を示す木構造に対して、通信相手の証明証を発行した証明機関から最上位の証明機関までのパス上にある機関証明証をすべて取り寄せて、それぞれについて検証処理を行うため、木構造で辿るパスの数だけの証明証の検証処理回数が必要となり、ユーザにとって大きな負担となっていた。また、木構造の上位の証明機関ほど、ユーザからの証明証取得要求が集中するため、上位証明機関におけるユーザからのアクセス要求に対する処理負荷が大きくなっていた。そこで、ユーザが少ない検証処理回数で通信相手の証明証

の正当性の確認及び特定の証明機関に対するユーザからのアクセス集中を回避する方法をこの発明は提案することを目的とする。

【0009】

【課題を解決するための手段】この発明では、直接信頼の上下関係がなかったために証明証の発行が行われていなかった証明機関に対して、従来はユーザが木構造を辿りながら行っていた検証処理を証明機関が自ら行って、その証明機関の公開鍵の正当性を確認することで、これを証明機関間の間接認証としてその証明機関の公開鍵に対して機関証明証の発行を行う。

【0010】つまりこの発明によれば、複数の証明機関間に木構造などの信頼関係が構成され、第 1 利用者の公開鍵であることを第 1 証明機関が保証した公開鍵証明証を第 2 利用者が受け取り、その公開鍵証明証を検証する際に、第 2 利用者の公開鍵を保証している第 2 証明機関が上記第 1 証明機関と直接的には信頼関係にない場合は、上記第 2 証明機関が上記第 1 証明機関の公開鍵の正当性の検証を行い、その検証結果を上記第 1 証明機関に対する機関証明証として発行し、第 2 利用者はその機関証明証内にある第 2 証明機関が正当と認めた第 1 証明機関の公開鍵を用いて第 1 利用者の公開鍵証明証の検証を行う。

【0011】上記第 2 証明機関による第 1 証明機関の公開鍵の正当性の検証は、その第 1 証明機関の公開鍵を保証しているその上位の証明機関の機関証明証を検証し、更にその上位証明機関の公開鍵の正当性を更にその上位証明機関が発行しているその機関証明証を検証するということにより順次木構造を辿って、最上位の証明機関が発行した機関証明証の検証まで行うことにより達成する。

【0012】1 度この検証を行い、正当であった場合は、その各機関証明証を第 2 証明機関に記憶しておき、他の証明機関の公開鍵の正当性を検証する場合に、まず、自己の証明機関内に、その他の証明機関の公開鍵を検証した機関証明証があるかを参照し、あればこれを用いる。

【0013】

【発明の実施の形態】図 1A にこの発明の実施例を適用したシステム例を示し、図 4A と対応する部分に同一符号を付けてある。従来技術での説明例と同様に、ユーザ A が署名文書 13 をユーザ B へ送るため、証明機関 CA1 が署名したユーザ公開鍵証明証 11A をユーザ B の端末 14B へ送信する。ユーザ B の端末 14B では受信した鍵証明証 11A は証明機関 CA1 が保証（署名）したものであるから、これの正当性を検証することはできない。

【0014】そこでユーザ B の端末 14B は証明機関 CA1 の公開鍵の信頼性検証を自己の証明機関 CA2 に依頼する。この依頼を受けた証明機関 CA2 は証明機関 CA1 からその信頼関係の木構造を辿って最上位の証明機

10

20

30

40

50

関CA5に達するまでのすべての証明機関の公開鍵検証に必要な機関証明証15₁₃、15₃₅を集め証明機関CA1の公開鍵に対する検証のために機関証明証15₁₃を機関証明証15₃₅内の証明機関CA3の公開鍵を用いて検証し、これに合格すると最上位証明機関CA5の公開鍵を用いて機関証明証15₃₅を検証する。

【0015】この検証に合格すれば、証明機関CA1に対して発行されている機関証明証15₁₃から証明機関CA1の公開鍵及び公開情報（機関名称など）を取り出す。その取り出した証明機関CA1の公開鍵及び公開情報と、証明機関CA2のこれらに対する署名とにより機関証明証15₁₂を作り、これをユーザBの端末14Bへ送信する。

【0016】以上のようにして端末14Bは証明機関CA2が発行した証明機関CA1の公開鍵に対する機関証明証15₁₂を取得し（S1）、端末14Bは図1Bに示すようにその機関証明証15₁₂を証明機関CA2の公開鍵12₂で検証し（S2）、合格したら、その機関証明証15₁₂に含まれている証明機関CA1の公開鍵を取り出し（S3）、これを用いて、ユーザAの端末14Aから受信した公開鍵証明証11Aを検証し（S4）、これに合格すれば、その公開鍵証明証11Aに含まれているユーザAの公開鍵を用いて受信した署名文書13の検証を行う（S5）。

【0017】証明機関CA2は以上のようにして証明機関CA1の公開鍵に対する機関証明証15₁₂を発行すると、これを記憶部に記憶しておき、同一の証明要求が発生した場合に、記憶した機関証明証を発行してもよい。また各検証済の機関証明証も記憶しておき、他の証明機関の公開鍵の検証で利用できるものは、それを利用して、検証処理を迅速化することもできる。証明機関CA1の公開鍵の正当性の検証は、機関証明証15₃₅を検証し、次に機関証明証15₁₃を検証するような順番としてもよい。

【0018】次に証明機関、例えばCA2が、これと直接信頼関係にない証明機関、例えばCA1の公開鍵の正当性を検証し、その証明証を発行する手順を図2を参照して説明する。ユーザから、対象証明機関（例えばCA1）の機関証明証発行依頼を受けると（S1）、その機関証明証について記憶部（データベース）21を検索し（S2）、既に発行済みの機関証明証であれば、これを記憶部21から読みだして、要求ユーザ端末へ送付する（S3）。

【0019】発行済みのものがなければ、その対象証明機関が発行した公開鍵証明証を参照し（S4）、その証明証を発行した証明機関を知り、かつその機関証明証を取得し（S5）、その発行証明機関より上位の証明機関

があるかを調べ（S6）、あればステップS5に戻って、その機関証明証を発行した証明機関を知るとともにその機関証明証を取得し、機関証明証を発行した証明機関が最上位に到達すると、それまでに取得した機関証明証の検証処理に移る。

【0020】つまり対象証明機関に対する機関証明証の署名を、その2の証明証を発行した証明機関に対する機関証明証内にある公開鍵で検証し（S7）、更にその発行証明機関の機関証明証の署名を、その証明証を発行した証明機関に対する機関証明証内の公開鍵を用いて検証し（S8）、機関証明証の署名の検証が最上位の証明機関の公開鍵により行ったかを調べ（S9）、そうでなければステップS8に戻り、機関証明証の署名の検証を順次上位の証明機関について行い、最上位の証明機関の公開鍵による検証が行われ、全ての検証に合格すると、対象証明機関に対する機関証明証からその対象証明機関の公開鍵及び公開情報を取り出し（S10）、その取り出した公開鍵及び公開情報に、これに対する自証明機関の署名を付けて機関証明証を作成して記憶部21に記憶するとともに要求ユーザ端末へ送信する（S11）。

【0021】

【発明の効果】以上述べたようにこの発明によれば、
① ユーザが、自分の証明証を発行した証明機関と異なる証明機関から発行されている通信相手の公開鍵証明証の正当性を検証する際に、そのユーザ端末自身で信頼の木構造を順次辿って複数の証明証を検証することなく、各証明機関が発行する間接認証による証明証のみを用いて確実に検証できることから、ユーザの検証処理が軽減される。

【0022】さらに、

② ユーザが検証処理の際に用いる間接認証による証明証の取得要求は、ユーザ自身の証明証の発行元証明機関のみに対して行われることから、木構造の上位の証明機関にアクセスが集中することを回避することができる。

【図面の簡単な説明】

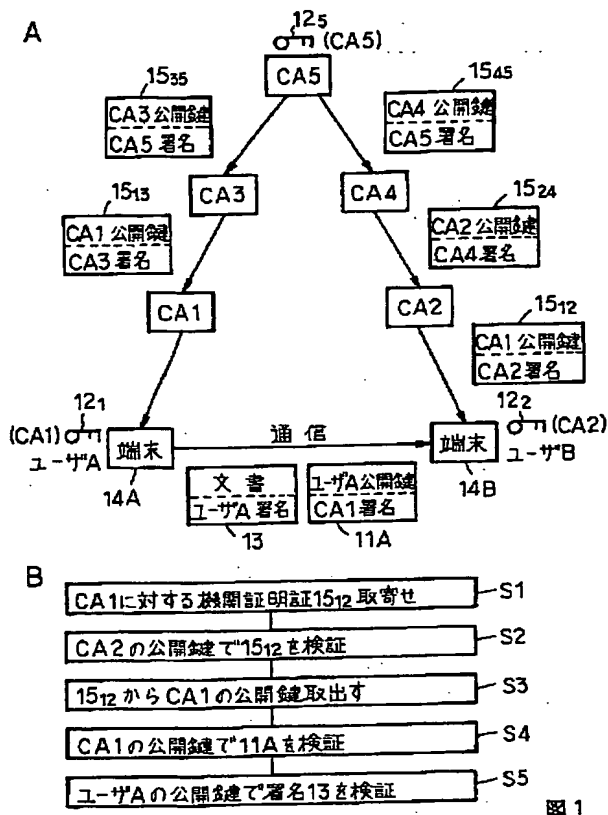
【図1】Aはこの発明を適用したシステム構成例を示すブロック図、Bはユーザ端末14Bの認証処理手順の例を示す流れ図である。

【図2】この発明において証明機関の公開鍵の認証要求を受けた証明機関の処理手順の例を示す流れ図。

【図3】同一の証明機関が発行した公開鍵証明証でのユーザ間通信における認証を説明するためのシステム構成例を示すブロック図。

【図4】Aは異なる証明機関により認証された公開鍵証明証によるユーザ間の通信における認証を説明するためのシステム構成例を示す図、Bはその公開鍵認証手順の例を示す図である。

【図1】



【図3】

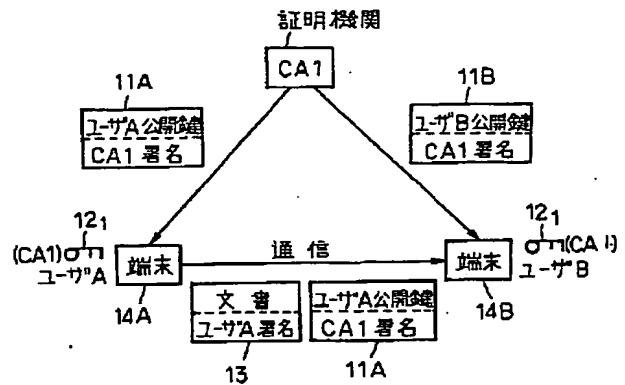
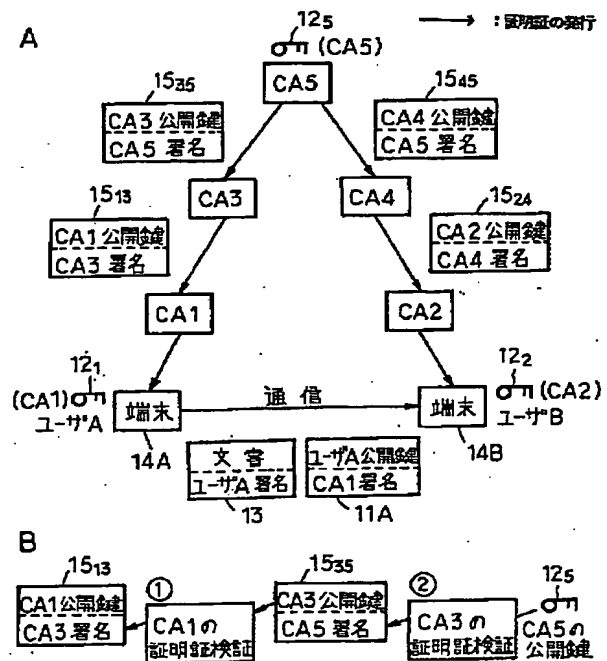


図3

【図4】



【図2】

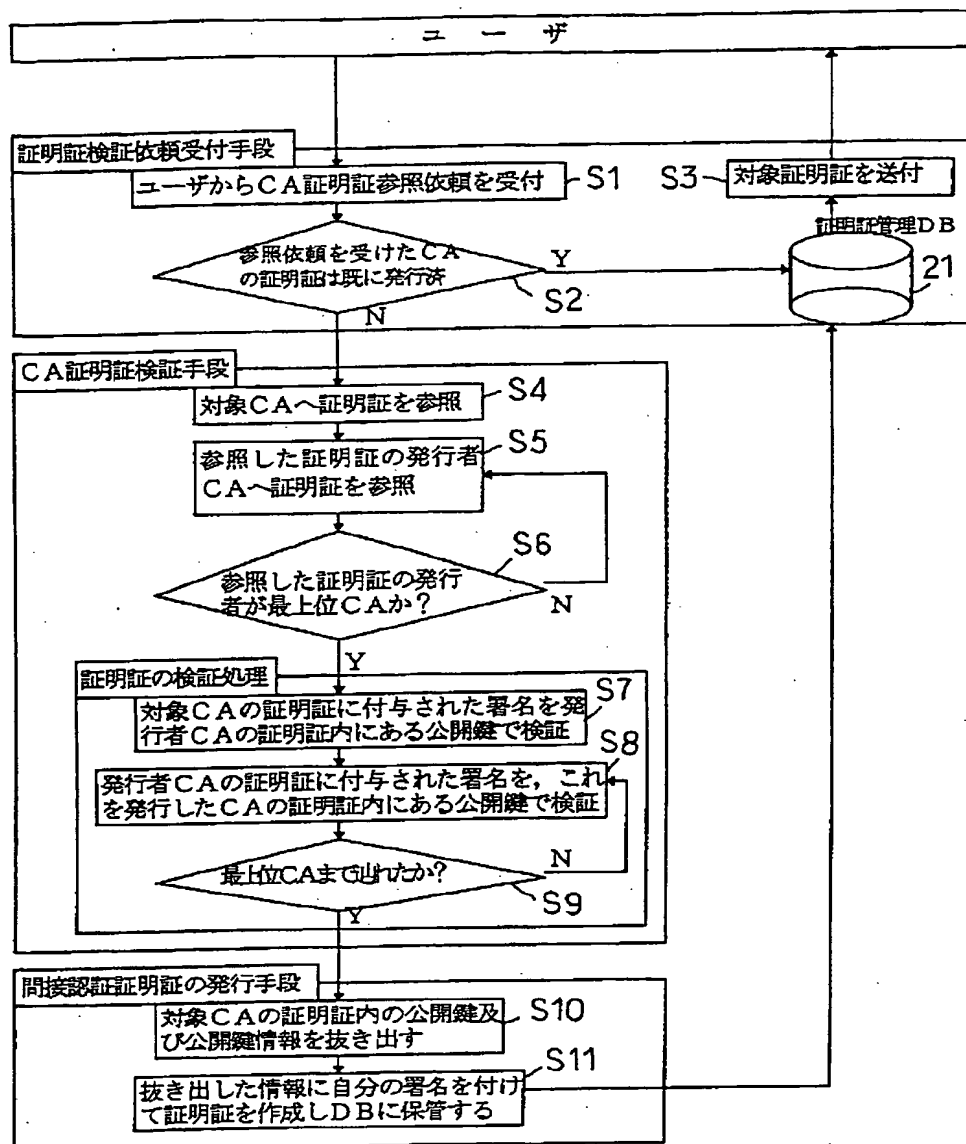


図 2